epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

CONSUMER FINANCIAL PROTECTION BUREAU

On the Consumer Financial Data Rights Rulemaking

January 25, 2023

The Electronic Privacy Information Center (EPIC) submits these comments in response to the Consumer Financial Protection Bureau (CFPB or the Bureau)'s Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights Outline of Proposals and Alternatives Under Consideration (Outline) published on October 27, 2022.

EPIC is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. EPIC has long advocated for privacy rights, data minimization, and algorithmic accountability and against the secret scoring of consumers.[1]

EPIC urges the CFPB to promulgate rules that will facilitate frictionless access by consumers to their own financial information; empower consumers to understand and control who has access to

[1] *See* EPIC, *In re Rocket* Money (Dec. 2022), https://epic.org/documents/epic-cfpb-complaint-rocket-money/; EPIC, Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem, FTC Commercial Surveillance ANPRM, R111004 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf; Consumer Reports and EPIC, How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking (Jan. 26, 2022), https://epic.org/wpcontent/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf; EPIC Statement to U.S. House Committee on House Administration, Hearing on "Big Data: Privacy Risks and Needed Reforms in the Public and Private Sectors" (Feb. 16, 2022), https://epic.org/documents/hearing-on-big-data-privacy-risks-and-needed-reforms-in-the-public-and-private-sectors/; EPIC Comments on CFPB Inquiry Into Big Tech Payment Platforms, CFPB-2021-0017 (Dec.2021), https://epic.org/documents/epic-comments-on-cfpb-inquiry-into-big-tech-payment-platforms/; *see generally*, EPIC, *Data Brokers*, https://epic.org/issues/consumer-privacy/data-brokers/ (last visited Mar. 23, 2022).

their personal data and for what purposes they may use it; and prohibit third parties from collecting, using, or retaining personal information beyond what is reasonably necessary to provide a product or service the consumer has requested.

EPIC's comment, which responds to questions from throughout the CFPB's Outline, is organized into the following topics: data minimization, ongoing use and retention of data, consumer rights, screen scraping, account verification, and data security.

I. Data Minimization

EPIC strongly supports the CFPB's proposed restrictions on third parties' collection, use, and retention of consumer-authorized information. EPIC has long highlighted the importance of data minimization: it is the most effective policy tool available to protect consumers' privacy, adhere to consumers' expectations, and safeguard personal information. EPIC has previously advocated for regulatory approaches based on data minimization, including in a 2022 white paper co-authored with Consumer Reports[2] and in our recent comments concerning the Federal Trade Commission's proposed rulemaking on commercial surveillance and data security.[3]

The following recommendation is responsive to Question 88.

EPIC supports the Bureau's proposal to limit the collection, use, and retention of consumer authorized-information to what is reasonably necessary to provide the product or service the consumer has requested. Imposing this data minimization standard would provide robust protections for consumers' financial information. In addition to this baseline standard, Bureau may establish heightened restrictions on the collection, use, and retention of especially sensitive information.

---

[2] EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[3] EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, Commercial Surveillance ANPR, R111004 (Nov. 2022, https://epic.org/documents/disrupting-data-abuse-protecting-consumers-from-commercial-surveillance-in-the-online-ecosystem/.

The CFPB should look to Title I, Sections 101-104 of the proposed American Data Privacy and Protection Act (ADPPA) for guidance in crafting a strong data minimization and purpose limitation standard.[4] EPIC also recommends that the Bureau take account of the data minimization standard laid out in the white paper EPIC co-authored with Consumer Reports.[5] Much like the CFPB's proposal, the rule that EPIC and Consumer Reports recommend would prohibit all secondary data uses with limited exceptions, limiting the collection and use of personal information to that which is reasonably necessary to provide the product or service that a consumer requested.[6]

The following recommendation is responsive to Question 89.

The Bureau correctly notes that sensitive personal information is especially likely to cause harm to individuals if exposed or misused. The baseline limitation standard is appropriate for many types of consumer data. However, we recommend that the Bureau impose a more exacting standard for sensitive information, limiting authorized third parties' collection of sensitive consumer data to what is *strictly* necessary to provide the product or service the consumer has requested (i.e., data without which it is impossible to provide such product or service).

The following recommendation is responsive to Question 91.

EPIC supports limiting the duration and frequency of third-party access to data according to what is reasonably necessary to provide the product or service the consumer has requested. Establishing a uniform standard for duration and frequency will increase the protection of personal data and decrease compliance costs, as (particularly smaller) firms will have clear guidance with respect to their obligations and will not need to shoulder the costs associated with multiple standards.

---

[4] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. Title I (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.
[5] EPIC and Consumer Reports, *How the FTC Can Mandate Data Minimization Through a Section 5 Unfairness Rulemaking*, (Jan. 26, 2022), https://epic.org/wp-content/uploads/2022/01/CR_Epic_FTCDataMinimization_012522_VF_.pdf.
[6] *Id.*

Indeed, a controller does not need to expend resources to safeguard data that it had never collected or that it has already deleted.

The following recommendation is responsive to Question 98.

The CFPB should adopt the first approach: prohibiting all secondary uses that are not reasonably necessary to provide the product or service requested. This is a privacy protective approach that incorporates data minimization and purpose specification standards and provides controllers with the clearest guidance. This approach also allows for certain secondary uses—such as fraud prevention and security—when they are reasonably necessary to provide the product or service requested. The last approach, prohibiting a secondary use only if the consumer has opted out, will not adequately protect consumers' privacy. An opt-out approach to secondary use restrictions will place an unreasonable burden on consumers by forcing them to manage confusing, innumerable, and ever-changing settings. The CFPB should not adopt a framework that provides privacy in name only.

The following recommendation is responsive to Question 99.

The CFPB should not adopt an opt-out approach for its rule. As noted, opt-out schemes routinely fail to protect consumers' privacy because they are difficult for consumers to use and understand (if consumers are aware of their existence to begin with). As a result, many consumers do not exercise their opt-out rights, and those that do are often forced to expend significant time and energy to protect their privacy.[7] Instead, the CFPB should adopt the first approach: by prohibiting

[7] *See* Hana Habib, et al., *An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites*, Proceedings of the 15th Symposium on Usable Privacy and Security (SOUPS 2019) 387-406 (2019), https://www.ftc.gov/system/files/documents/public_events/1548288/privacycon-2020-hana_habib.pdf ("This heuristic evaluation identified substantial issues that likely make exercising these privacy choices on many websites difficult and confusing for US-based consumers. Even though the majority of analyzed websites offered privacy choices, they were located inconsistently across websites. Furthermore, some privacy choices were rendered unusable by missing or unhelpful information, or by links that did not lead to the stated choice."); Claire Park, *How "Notice and Consent" Fails to Protect Our Privacy*, New America (Mar. 23, 2020), https://www.newamerica.org/oti/blog/how-notice-and-consent-fails-to-protect-our-privacy/.

secondary uses other than those which are reasonably necessary to provide a requested product or service, the limitation standard provides the most tailored and robust approach.

The following recommendation is responsive to Question 102.

The rule should not allow consumer data that has been nominally "deidentified" to be used by third parties beyond what is reasonably necessary. Reidentification is both possible and common[8] and poses a grave threat to consumers' financial information. At most, only information that has been anonymized to a high degree of certainty—as ADPPA describes it, "information [that] cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual"[9]—should be available for non-necessary secondary uses.

The following recommendation is responsive to Question 103.

EPIC supports the limits on retention that the CFPB is considering. This is a highly effective way to protect consumers' financial information: data that has been deleted is not at risk of misuse or breach. This rule may in fact reduce costs for small entities because they will not need to expend resources to safeguard data that they are required to delete.

II. Ongoing Use and Retention of Data

In managing their finances, consumers are barraged with advertisements for online tools for budgeting, investing, and spending. Many tools offer benefits for no direct monetary cost yet acquire, sell, and repurpose sensitive and granular data about consumers. Due to the endless variety of these tools and the complex interactions between them, consumers often do not have a clear

[8] *See* Natasha Lomas, *Researchers spotlight the lie of 'anonymous' data*, TechCrunch (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/ ("Researchers from two universities in Europe have published a method they say is able to correctly re-identify 99.98% of individuals in anonymized data sets with just 15 demographic attributes."); *See* Danny Bradbury, *De-identify, re-identify: Anonymised data's dirty little secret*, The Register (Sept. 16, 2021), https://www.theregister.com/2021/09/16/anonymising_data_feature/ "With a little work, people can often recreate your identity from these remaining data points. This process is called re-identification, and it can ruin lives.").

[9] ADPPA § 2(12(A)).

picture of what personal data is collected and how it is maintained or shared. EPIC is encouraged by many of the CFPB's regulatory proposals to address these problems and offers responses to several of the Bureau's questions below.

The following recommendations are responsive to Questions 103 and 104.

An authorized third party should be required to both affirmatively delete consumer data that is no longer reasonably necessary for providing the consumer's requested product or service *and* delete consumer data upon request. There should be no exceptions to deletion requirements outside of compliance with other laws and regulations. This is essential to maintain consumers' autonomy, which includes control over which entities can access and retain their data.

The following recommendations are responsive to Questions 117 and 118.

EPIC agrees that third parties should be obligated to regularly and clearly communicate essential information to the consumer about what data they collect, process, and retain. These disclosures should be made at least yearly and transmitted (at a minimum) via the primary means of communication between the consumer and the third party (e.g., by e-mail or in-app notice). Apart from these regular notices, authorized third parties must also be required to maintain a frictionless and conspicuous mechanism for the consumer to request information about the extent and purposes of the third party's access.

The following recommendations are responsive to Questions 92 and 93.

Although EPIC does not take a position on the permissible duration and frequency of third-party access to consumer-authorized information, EPIC agrees that the CFPB should establish such limits. EPIC also supports a requirement that third parties obtain reauthorization after a significant durational period has lapsed. The required schedule of reauthorizations should incorporate both a baseline frequency (for example, at least once a year) and a requirement that third parties seek

reauthorization sooner if a consumer has not interacted with the third party for an extended period (for example, six months).

III. Consumer Rights

The CFPB should strive to create an environment that ensures the efficacy of consumer data rights. From initially communicating data rights to actually exercising them, it is crucial that data providers are required to meaningfully disclose necessary information. EPIC is encouraged by the CFPB's proposed framework for consumer rights and offers recommendations below concerning required disclosures, communicating data rights, and revoking third party authorization.

The following recommendations are responsive to Questions 22-23, 30-31, and 37.

We applaud the CFPB for emphasizing the importance of requiring data providers to make critical information available to consumers about their financial products and services. EPIC will offer specific recommendations for the six non-exhaustive categories of information data providers are required to make available and the statutory exceptions to making that information available, followed by suggesting general principles for rulemaking in this area.

Category five, "Account identity information," should include information about the standard for identity verification services.[10] Due to the sensitive nature of this data, EPIC urges the CFPB to implement a strictly necessary standard for identity verification services. Moreover, the CFPB should integrate purpose specification principles into the required disclosures. If consumer data is collected and processed for more than one purpose, data providers should specify unrelated purposes to allow consumers to approve each individual unrelated purpose.

[10] CFPB, *Small Business Advisory Review Panel for Required Rulemaking on Personal Financial Data Rights: Outline of Proposals and Alternatives Under Consideration* 18 (Oct. 27, 2022) [hereinafter *SBREFA*], https://files.consumerfinance.gov/f/documents/cfpb_data-rights-rulemaking-1033-SBREFA_outline_2022-10.pdf.

With respect to the statutory exceptions to making information available, the CFPB should narrow or define the scope of certain terms. EPIC encourages the CFPB not to interpret the statutory exceptions in an overbroad way that would curtail consumer rights. First, the CFPB should define the scope of the exception permitting a data provider not to make any confidential commercial information available. Although a data provider may not be required to disclose "an algorithm used to derive credit scores or other risk scores or predictors,"[11] that definition should not preclude the CFPB from requiring data providers to disclose *when* they use an algorithm for those purposes or certain basic information about the function, inputs, and outputs of those algorithms. Second, the CFPB should narrow or define the scope of "any information that the data provider cannot retrieve in the ordinary course of its business with respect to that information."[12] Specifically, if the CFPB does not precisely define or narrow the term "ordinary course of business," it could be used over-inclusively to allow loopholes or shield data providers from disclosing information that they would otherwise be required to disclose.

In determining the categories of information data providers should disclose, the CFPB should recognize that a robust notice and transparency mechanism is necessary for consumers to understand and exercise their financial data rights. However, even the most effective notice and transparency schemes on their own cannot protect against personal or financial data abuse.[13] To alleviate the burden of risk mitigation on consumers, the CFPB should (as previously noted) establish substantive limits on financial data collection, processing, and retention.

Requiring data providers to disclose certain categories of information will benefit personal financial data rights in many ways. First, meaningful transparency can demonstrate that covered data

[11] *Id*. at 24.
[12] *Id*.
[13] *See* Philipp Hacker & Bilyana Petkova, *Reining in the Big Promise of Big Data: Transparency, Inequality, and New Regulatory Frontiers*, 15 Nw. J. Tech. & Intell. Prop. 1, 16–9 (2017) (discussing limits of transparency as accountability and consumer disclosure involving Big Data).

providers have evaluated the risks of processing personal financial data. In turn, consumers can better understand what financial data is being collected and processed, enabling them to exercise their available data rights. Otherwise, consumers can be harmed by losing control over the use of their financial data, often leading to diminished autonomy. If individuals are not informed about their data rights or how their financial data is being used, they lose the ability to exercise those rights effectively or make meaningful decisions.[14] Moreover, insufficient transparency or secrecy can result in myriad harms, from emotional and discriminatory harms to the breach, wrongful disclosure, or improper primary or secondary use of financial data.[15]

Second, the CFPB should strive to require that the six (or more) categories of information foster uniform disclosure. Categories of information should be designed to make the required disclosures as effective as possible. Privacy policies offer a cautionary tale: a 2019 survey of 150 privacy policies found that their disclosure of data processing activities was "vague," "opaque," and an "incomprehensible disaster."[16] If the CFPB fails to clearly categorize and define the information that data providers are required to make available, it may undermine the value of the information disclosed. Therefore, the CFPB should design the categories and data elements with precision to achieve uniform, effective disclosures.

The following recommendations are responsive to Question 87.

It is vital that data providers communicate disclosure obligations effectively to consumers. For consumers to exercise their data rights, they must understand the rights afforded to them under

[14] Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U.L. Rev. Online 793, 849 (2021), https://www.bu.edu/bulawreview/files/2022/04/CITRON-SOLOVE.pdf.
[15] *See id*. at 830–61.
[16] Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. Times (June 12, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html; *see also Social Media Privacy*, EPIC (2022), https://epic.org/issues/consumer-privacy/social-media-privacy/ ("[T]hese policies are often vague, hard to interpret, full of loopholes, subject to unilateral changes by the platforms, and difficult or impossible for injured users to enforce.")

the rule and how to exercise them in a timely manner. The notice should be clear, concise, conspicuous, and not misleading. Additionally, it must be readily accessible to the consumer in a way that reasonably reflects the context and relationship between the consumer and the data provider.

The following recommendations are responsive to Questions 94-95 and 97.

EPIC urges the CFPB to incorporate the requirement for authorized third parties to "provide consumers with a simple way to revoke authorization at any point, consistent with the consumer's mode of authorization."[17] Consumers should have the ability to control which third parties have access to their personal financial information and to withdraw authorization. To address various use cases within a single third party authorization, a third party could employ a simple series of check boxes identifying discrete uses of data that a consumer could toggle at any time for revocation.

IV. Screen Scraping

We support the Bureau's proposal to mandate that data providers develop third-party access portals. Screen scraping poses three significant risks to consumer privacy. First, a third party's possession of a consumer's access credentials risks misuse of those credentials by the third party. Second, the third party's collection and storage of many consumers' access credentials creates a target for hackers. Third, because data providers cannot control what information third parties scrape, scraping gives third parties access to all of the information in a consumer's account until the consumer changes their credentials. Scrapers could thus collect far more data than a consumer authorizes. Third-party access portals, on the other hand, allow data providers to technologically implement the data minimization and access rules the Bureau adopts in this rulemaking. Data that is never collected cannot be misused. The Bureau should require that data providers develop third-

[17] SBREFA, *supra* note 10, at 42.

party access portals on the quickest timeline and that these portals provide third parties access only to data within the scope of the consumer's authorization.

The following recommendations are responsive to Question 50 and 57.

We support the CFPB's third-party access portal proposal. Screen scraping creates privacy and security risks as described above. Through third-party access portals, consumers can allow third parties to access their data without handing over their credentials and data providers can limit and monitor third party data access. The Bureau should require data providers to develop these third-party access portals and use them to ensure that third parties are only able to access data within the scope of the consumers' authorization.

The CFPB could also promote adoption of a standard and open API and a standard authorization protocol to reduce reliance on data aggregators. Currently, data aggregators such as Plaid and Yodlee facilitate the vast majority of data transfers between data providers and third-party apps. These data aggregators came to prominence by translating data providers' many and disparate data structures—provided either through proprietary APIs or screen scraping—into standard APIs. But these companies have also been accused of violating customers' privacy, including selling consumer data without consent.[18] The CFPB's proposed rules should encourage development of standards that make it easier for third-party app developers to access consumer data directly from data providers to reduce reliance on major data aggregators.

[18] *See, g.g.*, Samantha Hawkins, *Plaid to Pay $58 Million to Settle Data Privacy Class Action*, Bloomberg Law (July 21, 2022), https://news.bloomberglaw.com/privacy-and-data-security/plaid-to-pay-58-million-to-settle-data-privacy-class-action; Corrado Rizzi, *Yodlee Hit with Privacy Class Action Over Alleged Behind-the-Scenes Sale of Sensitive Consumer Financial Data*, ClassAction.org (Aug. 25, 2020), https://www.classaction.org/news/yodlee-hit-with-privacy-class-action-over-alleged-behind-the-scenes-sale-of-sensitive-consumer-financial-data.

The following recommendations are responsive to Question 52–54, 56, and 78.

Because of screen scraping's security and privacy risks, the CFPB should require all data providers to develop third-party access portals on the quickest possible timeline. If the CFPB decides to allow scraping at all, it should only be temporary (used only until a third-party access portal is developed) and be accompanied by strict limits. If there is a feasible alternative or enhancement to credential-based screen scraping—such as a token authorization system—the CFPB should mandate that data providers implement such a system. Data providers should be required to use tokens to limit access frequency and duration to the scope of the consumers' authorization. It is important to note, however, that the data providers will not be able to limit the amount or types of data a scraper collects. Any third party that will or has in the past collected consumer credentials should be required to store the credentials in an encrypted format, inform the consumer that their credentials are currently stored, to provide the consumer with a method to delete their credentials, and to otherwise delete the credentials as soon as they are no longer necessary or within 30 days of the consumer's last login, whichever comes first.

The following recommendations are responsive to Question 90 and 109.

As explained above, if the CFPB allows scraping at all, it should only allow data providers to make scraping a temporary measure for complying with its rules while the data provider develops a third-party access portal. This is because the data provider is not able to technologically limit the amount or type of data the third party accesses through scraping. Instead, it is up to the third party to either design a scraper that collects only data within the consumers' authorization—which can be difficult to implement—or, after collecting more data than the consumer authorized, immediately delete the data it was not authorized to collect. Such data practices invite misuse. But if the CFPB decides to allow scraping as a temporary measure, it should require that third parties that use scraping design their scrapers, to the maximum extent possible, to collect only data that is strictly

necessary and within the consumers' authorization, and to immediately delete data they collect beyond those limits.

V. Account Verification

We applaud the Bureau for emphasizing the need to safeguard against unauthorized disclosure of consumer account information. As was evident nearly twenty years ago in the context of phone subscriber records, inadequate account verification procedures can result in privacy harms,[19] such as recent unauthorized access by data brokers, private investigators, and others.[20] Hackers have similarly utilized fraudulent emergency data access requests to obtain private consumer data.[21] The Gramm-Leach-Bliley Act prohibited attempts to obtain consumer financial information under false pretenses;[22] however, unlike the rules for phone subscriber records which focus on the provider rather than on the fraudster, liability for the financial institution which wrongly disclosed the information is covered only indirectly and not within the same provision.[23] Greater attention from the CFPB to account verification procedures can prevent repeated, avoidable consumer harms like these in the future.

[19] *See* Petition of EPIC for Rulemaking to Enhance Security and Authentication Standards For Access to Customer Proprietary Network Information, *In re* Implementation of the Telecommunications Act of 1996, CC Docket No. 96-115 (filed Aug. 30, 2005), https://www.fcc.gov/ecfs/search/search-filings/filing/5513305577.
[20] *See* FCC Proposes Over $200M in Fines for Wireless Location Data Violations (Feb. 28, 2020), https://www.fcc.gov/document/fcc-proposes-over-200m-fines-wireless-location-data-violations.
[21] *See Hackers Gaining Power of Subpoena Via Fake "Emergency Data Requests"*, Krebs on Security (Mar. 29, 2022), https://krebsonsecurity.com/2022/03/hackers-gaining-power-of-subpoena-via-fake-emergency-data-requests/; William Turnton, Apple and Meta Gave User Data to Hackers Who Used Forged Legal Requests, Bloomberg (updated March 30, 2022, 3:30 PM), https://www.bloomberg.com/news/articles/2022-03-30/apple-meta-gave-user-data-to-hackers-who-forged-legal-requests.
[22] FTC, Gramm-Leach-Bliley Act, https://www.ftc.gov/legal-library/browse/statutes/gramm-leach-bliley-act (Subtitle B, codified as 15 USC 6821) (last accessed Jan. 25, 2023).
[23] Either under the GLBA's privacy rule, as the consumer information was shared with a third party undisclosed in the data provider's privacy policy, or insofar as the unauthorized access occurred as a result of violations of data security practices required under the Safeguards Rule.

The following recommendations are responsive to Questions 26-27, 39, 71, and 75.

We urge the Bureau to make explicit that companies subject to its authority under Section 1033 will be held to a standard no less than those established by the most recent updates to the Safeguards Rule.[24] For example, the Bureau should prohibit mere biographic identifiers (e.g. date of birth, Social Security Number, etc.) to suffice for account verification,[25] requiring additional measures such as multi-factor authentication when purported consumers attempt to access their account information. The Bureau should also require providers to (1) minimize employee access to consumer data, as employees including customer service staff may be in a position to approve or deny access to consumer data by purported consumers; (2) implement audit trails to facilitate investigating a breach after the fact, where verification processes failed to prevent unauthorized access; and (3) encrypt data to mitigate harm resulting from attempts to circumvent these access controls. The latest updates to the Safeguards Rule, which take effect in June 2023, include requirements that align with these recommendations and apply to all covered financial institutions, regardless of size. For financial institutions that maintain consumer data on 5,000 or more individuals, all of the Safeguards Rule's requirements apply, including risk assessments, penetration testing, and ongoing monitoring.[26]

The CFPB might also draw inspiration from the Federal Trade Commission's enforcement efforts in data security matters (for example, requiring companies to provide security notifications to

[24] 16 C.F.R. § 314.
[25] This is standard practice in the context of phone subscriber data. *See, e.g.*, 47 CFR § 64.2010 (c) (requiring telecommunications carrier to authenticate customer without use of readily available biographical information, or account information, prior to allowing customer online access to CPNI related to account). In terms of harms that can result from permitting authentication using biographic information, in late 2020, websites used to generate auto insurance quotes were exploited to obtain personal data by using biographic identifiers. *See* Industry Letter Re: Cyber Fraud Alert, N.Y. State Dep't of Fin. Servs., Cybersecurity Div. (Feb. 16, 2021), https://www.dfs.ny.gov/industry_guidance/industry_letters/il20210216_cyber_fraud_alert.
[26] Addressed further in Section VI, *infra*.

consumers when login credentials are changed)[27] as well as requiring companies to invalidate breached authentication data for user verification purposes to avoid misuse by bad actors.[28]

The following recommendations are responsive to Questions 72, 73-75, and 80-81.

We support the CFPB's proposals to require data providers to verify the third party's authorization to access that consumer's data, as well as to authenticate the identity of the third party and the scope of data requested, before sharing consumer data. We also support the CFPB's proposal to require providers to obtain consumer confirmation of third-party access requests and to allow an easy method for consumers to revoke their authorization and terminate third party access. We further urge the CFPB to require companies subject to its 1033 authority to establish procedures for verifying the validity of data access requests that appear to result from lawful process, to prevent fraudulent data access requests.

Consumer protection agencies at all levels of government consistently encourage consumers who suspect they are the target of attempted government impersonation fraud to hang up the phone (or ignore the text/email), go to the agency's .gov website, and use the contact information provided there to seek clarification.[29] Companies entrusted with consumer data should be held to at least this minimal standard when deciding how to respond to a request for consumer data from a third party or to an emergency data access request from a government entity. Even emergency requests from

[27] Complaint, *In re Paypal, Inc.*, FTC File No. 162-3102 at ¶ 40(c)(1) (May. 24, 2018), https://www.ftc.gov/legal-library/browse/cases-proceedings/162-3102-paypal-inc-matter.
[28] Complaint, *In re Residual Pumpkin Entity, LLC, d/b/a CafePress*, FTC File No. 1923209 at ¶ 25 (Jun. 23, 2022), https://www.ftc.gov/legal-library/browse/cases-proceedings/1923209-cafepress-matter.
[29] *See, e.g.*, *Fraud Alert – May 5, 2022*, State of California Department of Consumer Affairs, https://www.dca.ca.gov/licensees/scam_alert.shtml (last accessed Jan. 24, 2023); *SCAM ALERT: LA County Will Not Ask For your Info In Unexpected Phone Calls*, Los Angeles County Department of Consumer & Business Affairs (Feb. 11, 2022), https://dcba.lacounty.gov/newsroom/scam-alert-la-county-phone-spoofing-scam/; FTC Consumer Advice, *How to Avoid a Government Impersonator Scam*, https://consumer.ftc.gov/articles/how-avoid-government-impersonator-scam (last accessed Jan. 24, 2023).

federal agencies should not be excluded from this authentication/verification regime.[30] Data providers and third parties should establish and maintain communication and authorization verification channels to reduce the likelihood of imposters or otherwise unauthorized third parties obtaining access to consumer data.

The consumer should be in control of how often they must confirm authorization of third-party access to their data and how easily they can revoke that authorization. A similar model has been used for fraud prevention in the credit card context.[31] Customers should be able to set the triggers that require their confirmation of third-party access. Regarding revocation specifically, consumers may want to require multiple steps to prevent unintentional disruptions or may prefer it be as simple as texting "STOP" to a customer support number. The CFPB should allow consumers to revoke their authorization as easily as it was granted, while also allowing consumers to make revocation a more involved process if that is the consumer's preference.

The following recommendations are responsive to Questions 39-40.

Additionally, it is unrealistic to expect the average consumer to have the same technological safeguards as a financial institution. As such, companies should be required to provide a secure method for transferring the consumer's account data to another institution without requiring the consumer to download files locally. Companies should also be required to alert consumers of the risks of storing personal financial information in an unsecure folder on their computer or other

[30] *See, e.g.*, *DEA Investigating Breach of Law Enforcement Data Portal*, Krebs on Security (May 12, 2022), https://krebsonsecurity.com/2022/05/dea-investigating-breach-of-law-enforcement-data-portal/ (noting in the context of a DOJ database being hacked that "when hackers can plunder 16 law enforcement databases, arbitrarily send out law enforcement alerts for specific people or vehicles, or potentially disrupt ongoing law enforcement operations — all because someone stole, found or bought a username and password — it's time for drastic measures.").

[31] *See, e.g.*, Chauncey Crail and Caroline Lupini, *How to Enable Mobile Credit Card Alerts for Purchases and Fraud*, Forbes (Sept. 7, 2022 1:03pm), https://www.forbes.com/advisor/credit-cards/how-to-enable-mobile-credit-card-alerts-for-purchases-and-fraud/.

personal device and to provide this alert at the point at which a consumer is able to download their account information (e.g., as a .csv file).

VI. Data Security

Consumers face an epidemic of data breaches and resulting identity theft and harm due to a lack of investment in and commitment to data security.[32] Companies will not adequately invest in data security unless they face significant consequences for a failure to do so.[33]

We support the CFPB's proposal to require authorized third parties to "develop, implement, and maintain a comprehensive written data security program appropriate to the third party's size and complexity, and the volume and sensitivity of the consumer information at issue."[34] As we noted in our recent comments to the Federal Trade Commission,[35] data security measures should apply to companies at a level commensurate with the scope and scale of the type and volume of data they collect.[36] Given the sensitivity of personal financial data, we urge the CFPB to consider implementing standards similar to what we advocated to the Federal Trade Commission in our comments—including but not limited to access controls, secure password practices, user authentication, system segmentation, traffic monitoring, staying current on known vulnerabilities,

---

[32] *See, e.g.*, Verizon, *Financial Services Data Breaches*, https://www.verizon.com/business/resources/reports/dbir/2021/data-breach-statistics-by-industry/financial-services-data-breaches/ (last accessed Jan. 24, 2022); Paul Bischoff, *Financial data breaches accounted for 153.3 million leaked records from January 2018 to June 2022*, Comparitech (updated July 27, 2022), https://www.comparitech.com/blog/vpn-privacy/financial-data-breaches/.

[33] *See, e.g.*, Bruce Schneier, *The Uber Hack Exposes More Than Failed Data Security*, The New York Times (Sept. 26, 2022), https://www.nytimes.com/2022/09/26/opinion/uber-hack-data.html; Michael Kende, *How Secure Is Our Data, Really?*, MIT Press Reader (May 16, 2021), https://thereader.mitpress.mit.edu/how-secure-is-our-data-really/.

[34] *SBREFA*, *supra* note 10, at 46.

[35] *See* EPIC, *Disrupting Data Abuse: Protecting Consumers from Commercial Surveillance in the Online Ecosystem*, FTC Commercial Surveillance ANPRM, R111004 (Nov. 2022), https://epic.org/wp-content/uploads/2022/12/EPIC-FTC-commercial-surveillance-ANPRM-comments-Nov2022.pdf.

[36] *See, e.g.*, William McGeveran, *The Duty of Data Security*, 103 Minn. L. Rev. 1135, 1179 (2018), https://www.minnesotalawreview.org/wp-content/uploads/2019/02/1McGeveran_FINAL.pdf (noting that across multiple data security frameworks "the duty of data security scales up or down in proportion to the resources and risk profile of each data custodian").

security reviews, and employee training.[37] Much of this is already incorporated into the requirements of the updated Safeguards Rule which take effect this June.[38]

The following recommendations are responsive to Question 111.

We agree with the CFPB that the "adequacy of the security of third-party access portals could significantly impact consumer interests related to the privacy and security of their information and other sensitive information made available through such portals."[39] As we also noted in our recent comments to the Federal Trade Commission, per the Safeguards Rule, companies must use reasonable means to confirm that service providers or third parties with access to consumer data not merely implement but *actively maintain*[40] adequate safeguards to ensure the confidentiality and security of consumer data, as service providers can be a favored attack vector for malicious actors.[41] Consequently, the CFPB should be explicit that authorized third parties will be held accountable for any unauthorized disclosure of consumer data that occurs as a result of inadequate safeguards implemented by the third party's own service providers.

---

[37] *See Disrupting Data Abuse* at 181–216. As noted in EPIC's comments to the FTC, these are also consistent elements across FTC enforcement actions over the past 10 years, as well as various state data privacy and security laws, and frameworks. *See, e.g.*, id. at 199, 201–05.
[38] 16 C.F.R. § 314.
[39] *SBREFA*, *supra* note 10, at 35.
[40] Verizon consistently reports that 44% or more of organizations fail to maintain PCI-DSS compliance in between annual compliance validations (most recently more than 56% failed to maintain compliance). *See, e.g.*, Verizon, *2022 Payment Security Report* 82 (Sept. 2022), https://www.verizon.com/business/resources/T38f/reports/2022-payment-security-report.pdf.
[41] *See, e.g.*, *Standards for Safeguarding Customer Information*, 16 C.F.R. § 314.4(f) (2021), https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information (citing Kevin McCoy, *Target to Pay $18.5M for 2013 Data Breach that Affected 41 Million Consumers*, USA Today (May 23, 2017), https://www.usatoday.com/story/money/2017/05/23/target-pay-185m-2013-data-breach-affected-consumers/102063932/) ("For example, in 2013, attackers were reportedly able to use stolen credentials obtained from a third-party service provider to access a customer service database maintained by national retailer Target Corporation, resulting in the theft of information relating to 41 million customer payment card accounts."). Supply chain security literature suggests that third parties are often a preferred attack vector. *See, e.g.,* ABA Cybersecurity Legal Task Force, *Vendor Contracting Project: Cybersecurity Checklist Second Edition* 1 (2021), https://www.potteranderson.com/media/publication/941_Vendor%20Contracting%20Project%20-%20Cybersecurity%20Checklist.pdf; *Target Hackers Broke in Via HVAC Company*, Krebs on Security (Feb. 5, 2014), https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/.

The following recommendations are responsive to Questions 56 and 69-71.

Similarly, the CFPB should make explicit that authorized third parties will be liable for consumer credentials compromised from their systems. This will encourage third parties to retain the credentials for only as long as is strictly necessary. Regarding performance standards for authentication and for other cybersecurity measures, the CFPB could refer to NIST's Cybersecurity Framework[42]--note that updates to this framework are expected to be released soon[43]--or to similar frameworks from FINRA,[44] CISA,[45] or California's Department of Justice.[46]

The following recommendations are responsive to Questions 108 and 110.

As a data security matter, properly destroyed consumer data cannot be improperly accessed.[47] We support the CFPB's proposals to ensure authorized third parties do not retain consumer data beyond what the consumer intended to authorize—both in terms of the scope of the data retained and

[42] NIST, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; NIST, *Getting Started with the NIST Cybersecurity Framework: A Quickstart Guide* (Updated Apr. 19, 2022), https://csrc.nist.gov/Projects/cybersecurity-framework/nist-cybersecurity-framework-a-quick-start-guide (providing a helpful high-level overview).
[43] *See* NIST Cybersecurity Framework 2.0, https://www.nist.gov/system/files/documents/2022/10/03/NIST_CSF_update_Fact_Sheet.pdf (last accessed Jan. 25, 2023).
[44] FINRA, *Report on Cybersecurity Practices* (Feb 2015), https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf; FINRA, *Core Cybersecurity Threats and Effective Controls for Small Firms* (May 2022), https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf.
[45] CISA, *Cross-Sector Cybersecurity Performance Goals* (2022), https://www.cisa.gov/sites/default/files/publications/2022_00092_CISA_CPG_Report_508c.pdf
[46] In 2016, then-California Attorney General Kamala Harris also offered recommendations based on the CIS framework, which outlined explicitly parallel recommendations from NIST, ISO, HIPAA, FFIEC, and PCI DSS frameworks. *See* Kamala D. Harris, Attorney General, *California Data Breach Report* 31 (2016), https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf.
("The controls are intended to apply to organizations of all sizes and are designed to be implementable and scalable."); *id.* at Appendix B.
[47] 16 CFR 314.4(c)(6) (requiring deletion and periodic review of retention policies to minimize unnecessary retention).

the duration for which it is retained. Consumers can re-authorize access if the lapse in authorization was unintended.

Regarding dedentified consumer data, we encourage the CFPB to require a standard closer to anonymization than mere deidentification, which would greatly reduce the likelihood of reidentification of consumer data. This standard is much higher than merely requiring that names or exact birthdates be removed, that a simple cipher be applied to data, or that data be pseudonymized. EPIC suggests the following definition of deidentified data, adapted from the proposed American Data Privacy and Protection Act (ADPPA)[48]:

> DE-IDENTIFIED DATA.—The term ''de-identified data'' means information that does not identify and is not linked or reasonably linkable to a distinct individual or a device, regardless of whether the information is aggregated, and if the covered entity or service provider—
>
> (A) takes technical measures to ensure that the information cannot, at any point, be used to re-identify any individual or device that identifies or is linked or reasonably linkable to an individual;
>
> (B) publicly commits in a clear and conspicuous manner—
>
> (i) to process and transfer the information solely in a de-identified form without any reasonable means for re-identification; and
>
> (ii) to not attempt to re-identify the information with any individual or device that identifies or is linked or reasonably linkable to an individual; and
>
> (C) contractually obligates any person or entity that receives the information from the covered entity or service provider—
>
> (i) to comply with all of the provisions of this paragraph with respect to the information; and
>
> (ii) to require that such contractual obligations be included contractually in all subsequent instances for which the data may be received.

We support the CFPB's proposals to safeguard consumer data security, especially when entrusted to third parties. We urge the Bureau to consider how liability might best incentivize

[48] American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. § 2(12) (2022), https://www.congress.gov/bill/117th-congress/house-bill/8152/text.

companies to retain data for only as long as is necessary and to ensure that deidentified data stored beyond the maximum allowed retention period is truly incapable of being reidentified.

VII. Conclusion

We applaud the CFPB's thoughtful efforts to provide flexibility to consumers and increase competition in the marketplace without jeopardizing the privacy, integrity, or security of consumer data.

We appreciate this opportunity to comment and are willing to engage with the agency further on issues such as third-party authentication, consumer rights, data minimization, screen scraping, account verification, and data security. These issues relate closely to empowering consumers to understand and control who has access to their personal data and for what purposes they may use it, as well as to limiting third party collection and use of this data to only what is essential for fulfilling the consumer's requests.

Respectfully submitted,

/s/ Ben Winters
Ben Winters
Senior Counsel

/s/ John Davisson
John Davisson
Senior Counsel

/s/ *Megan Iorio*
Megan Iorio
Senior Counsel

/s/ *Calli Schroeder*
Calli Schroeder
Senior Counsel

/s/ *Sara Geoghegan*
Sara Geoghegan
Counsel

/s/ *Chris Frascella*
Chris Frascella
Law Fellow

/s/ *Suzanne Bernstein*
Suzanne Bernstein
Law Fellow